[**APPLICATION**] Enabling platform network stack control in a virtualization platform

US Pat. 10954905 - Filed Sep 30, 2004

TPM may aid in guarding secrets by communicating with a NIC. [0039] A hybrid **VMM** is an specialized class of **hypervisor** that leverages a dedicated guest OS **...**

[**APPLICATION**] Local secure service partitions for operating system security

US Pat. 11097697 - Filed Apr 1, 2005

In particular, the audit software 24 is modified to call an audit log service in partition 18 using a partition ID provided by **hypervisor** or **VMM** 12 from **TPM ...**

[**APPLICATION**] Methods and apparatus for defeating malware

US Pat. 11601321 - Filed Nov 16, 2006

In some embodiment, the VTA may itself be implemented as a **VMM** or a **hypervisor**. In one embodiment, the candidate code module to be checked for authorization **...**

[**APPLICATION**] Method and System for Implementing a Mobile Trusted Platform Module

US Pat. 11840823 - Filed Aug 17, 2007 - Fujitsu Limited

Some of these components, such as **TPM** device 2110 and interface 2120 are **...** In some embodiments **VMM** 2130 may comprise a **hypervisor** running multiple **...**

[**APPLICATION**] Methods and arrangements to launch trusted, co-existing environments

US Pat. 11527180 - Filed Sep 26, 2006

A key component of a trusted processing system is the **TPM**, **...** For instance, in some systems a virtual machine monitor (**VMM**) or **hypervisor** code may assume **...**

[**APPLICATION**] Method and apparatus for migrating virtual trusted platform modules

US Pat. 11512989 - Filed Aug 29, 2006

A **TPM** is a hardware component that resides within a processing system and provides **...** products such as a virtual machine monitor (**VMM**) or **hypervisor**. **...**

[**APPLICATION**] Method and apparatus for remotely provisioning software-based security ...

US Pat. 11171880 - Filed Jun 29, 2005

A **TPM** is a hardware component that resides within a processing system and provides

... products such as a virtual machine monitor (**VMM**) or **hypervisor**. ...

[**APPLICATION**] Method and apparatus for migrating software-based security coprocessors
US Pat. 11171134 - Filed Jun 29, 2005
A **TPM** is a hardware component that resides within a processing system and provides
... products such as a virtual machine monitor (**VMM**) or **hypervisor**. ...

[**APPLICATION**] Method and apparatus for providing software-based security coprocessors
US Pat. 11171133 - Filed Jun 29, 2005
A **TPM** is a hardware component that resides within a processing system and provides
... products such as a virtual machine monitor (**VMM**) or **hypervisor**. ...

[**APPLICATION**] Methods and apparatus for generating endorsement credentials for software ...
US Pat. 11171856 - Filed Jun 29, 2005
A **TPM** is a hardware component that resides within a processing system and provides
... products such as a virtual machine monitor (**VMM**) or **hypervisor**. ...

Stay up to date on these results using the patents RSS feed on **VMM TPM hypervisor**.

Google
Result Page: 1 2 **Next**